Repos-csel ： サイバーセキュリティeラーニングリポジトリの構築の提案

著者	上田 浩，後藤田 中，平岡 斉士，金子 晃介，中村 誠，松本 多恵，岡村 耕二，田口 雅晴，井上 俊治，中尾 礼文，石田 亮介
出版者	情報処理学会
雑誌名	情報処理学会研究報告
巻	2020-CLE-30
号	3
ページ	1-7
発行年	2020-03
URL	http://hdl.handle.net/10114/00022969

Repos-csel: サイバーセキュリティ e ラーニングリポジトリの構築の提案

上田 浩[1,a)]　後藤田 中[2]　平岡 斉士[3]　金子 晃介[4]　中村 誠[6]　松本 多恵[7]　岡村 耕二[5]　田口 雅晴[8]
井上 俊治[8]　中尾 礼文[8]　石田 亮介[8]

概要：我が国の大学等において，サイバーセキュリティ教育を e ラーニングで行うことは主に監督官庁からの通達に従う形で行われてきた．e ラーニングコースの開発には多大のコストを要するにも関わらず，アリバイ作り的な運用が散見される．加えて，そのようなコースが学習者の意欲を高めるものとなっておらず，それらを構成するコンテンツ，とりわけテストについて，一貫した設計・評価基準が適用されていないのが現状である．この問題意識のもと，著者らはサイエンティフィック・システム研究会 サイバーセキュリティ・情報倫理 e ラーニング教育の課題解決 WG における活動を通じ，より良いサイバーセキュリティ教育のためのテストを作成するため (1) 「知識」の有無ではなく，判断スキルの習得を前提とする「態度」獲得を目指した，インストラクショナル・デザインの考え方を取り入れる (2) 共有リポジトリを構築し，同じ課題を持つ関係者が共同で作問することを提案する．本提案は，著者らがこれまで取り組んできた，共通 LMS によるサイバーセキュリティ教育と比較して，各大学等の事情に応じて問題を取捨選択できること，各大学のプラットフォームを活用でき責任分界点が明確になるという利点があり，より持続的な取り組みを目指すものである．現在，Moodle 3.8.1 に StudentQuiz プラグインを導入したコースを共有リポジトリ Repos-csel(https://csel.media.hosei.ac.jp/) として公開している．同リポジトリにおいて，WG メンバーがテスト問題を作成・共有し，その評価を行う機能の検証を行っている．

キーワード：サイバーセキュリティ教育，e ラーニング，インストラクショナル・デザイン，共有リポジトリ，Moodle，StudentQuiz

Repos-csel: New proposal for Cybersecurity e-Learning Quiz Repository

Abstract: In this study, we propose two solutions to improve quiz for cyber security awareness education through activities in The Society of Scientific Systems : (1) Adopt Instructional Design to achieve not only knowledge, but an attitude that is able to learn ability to judge. (2) Shared repository to collaborate over institutions or organization. The motivation of this study is that, it is big challenge to provide good cyber security awareness e-learning for students in Japanese universities. Because learners has no positive attitude to such kind of e-learning in many cases and no one has clear and general criteria to evaluate the quiz, main content of e-learning course. Our proposal is sustainable and has advantage that each institution can make a choice quizzes from the repository circumstantially and can provide quizzes via own learning management system (LMS), compared with our recent work based on shared LMS. Currently, we, the member of the working group of cyber security e-learning of The Society of Scientific Systems, started make quizzes and upload them to the repository, Repos-csel(https://csel.media.hosei.ac.jp/), based on Moodle 3.8.1 and StudentQuiz Plugin.

Keywords: Cyber security awareness education, e-learning, Instructional design, Shared repository, Moodle, StudentQuiz

1. はじめに

我が国の大学等において，サイバーセキュリティ教育を e ラーニングで行うことは，情報セキュリティポリシーの整備，Learning Management System (LMS) などのプラットフォームの整備とほぼ同期して，主に監督官庁の通達に従う形で行われてきた．

とりわけ大学等における情報セキュリティポリシー整備は，筆者の経験では，国立大学が法人化された直後に文科省から発出された「情報セキュリティポリシーの策定」に関する調査が契機となったと記憶している．そのことは，多数の国立大学が「情報セキュリティポリシー」という文言を 2004〜2009 年度の第 1 期中期目標・中期計画に含めていることからも明白であろう．一方，情報セキュリティポリシーを策定した後，それをどのように実質化する，あるいは普及させるかという課題があり，文書による通知，対面の講習会などが行われていた．

このような教育は大学の正規の教育課程に組み入れることが望ましいが [1]，限られた単位の中で十分な時間を充てることが困難であることから，また学生だけでなく教職員への教育も行うために e ラーニングによる教育が採用されてきた．たとえば様々な大学で採用されている INFOSS 情報倫理[*1]，2002 年度に国立大学情報処理教育センター協議会とメディア教育開発センターの共同事業として始まった「情報倫理デジタルビデオ小品集」[2]，国立情報学研究所で制作された「ヒカリ& つばさの情報セキュリティ三択教室」[3]，群馬大学で開発され，NII により提供される「りんりん姫と学ぼう！情報倫理」[4]，九州大学で採用された，ゲーム感覚で情報セキュリティを学ぶ「シンプラ Z」[5]，東京大学で採用された「大学向け テストで学ぶ 情報セキュリティ」[6] などが挙げられる．

このような取り組みには少なくないコストが費やされているにもかかわらず，教育の実施，すなわち「受講率」にのみフォーカスが当てられ，その改善まで至らない状況が散見される．一方，サイバーセキュリティ教育に限らず，e ラーニングが学習者の意欲を高めるものになっていない場合があることは事実であり，改善が必要である．

1 法政大学 情報メディア教育研究センター
Research Center for Computing and Multimedia Studies, Hosei University, Koganei, Tokyo 184–8584, Japan
2 香川大学 総合情報センター
3 熊本大学 教授システム学研究センター
4 九州大学 サイバーセキュリティセンター
5 九州大学 情報基盤研究開発センター
6 東京大学 情報システム本部
7 島根大学 研究・学術情報機構 総合情報処理センター
8 富士通株式会社 文教・地域ソリューション事業本部
a) uep@hosei.ac.jp
*1 筆者の確認した範囲では筑波，和歌山，京都産業，中部，立正，高崎経済，三重，成蹊，鳥取，東京理科，電気通信の各大学で導入されている．発売元によると INFOSS とは Information Security をもとにした商標であるとのこと．

本稿は，このような取り組みを踏まえ，サイバーセキュリティ e ラーニングの課題解決を目指した共有リポジトリの構築を提案するものである．以下，2 節でサイバーセキュリティ e ラーニングの課題を提起し，3 節でその解決のための手法として，インストラクショナル・デザインを取り入れたコンテンツ開発とそれらを共有するリポジトリの構築を提案する．次いで 4 節でそのプロトタイプの実装と現状について報告し，5 節で全体をまとめ今後の展望を述べる．

2. 問題意識

これまで筆者らはそれぞれの所属でサイバーセキュリティ教育にかかわってきた．e ラーニングは対面教育の完全な代替にはなり得ないことは共通認識である．両者を比較して優劣を論ずるのではなく，オンライン教育でこそ可能な教育の実現方法があると考える．一方，これまでの経験から得られた，その課題と思われる事項を以下に列挙する．

受講率のみで評価するアリバイ作り的運用　著者らの所属機関では，サイバーセキュリティの e ラーニングコースについて，その教育的効果を評価することなく，受講者が何名で，受講率が低迷しているのが問題だという議論を数多く見てきた．e ラーニングによるサイバーセキュリティ教育には，少なくないコストが必要であるにも関わらず，アリバイ作りになっていると言わざるを得ない．

受講者に合わせることが困難　大学生は初・中等教育においてある程度のサイバーセキュリティに関する教育を受けているはずであるが，その習熟度合いは一定ではなく，前提知識が一定ではない．受講者に合わせた e ラーニングを実現すること，それが適切かどうかの評価が困難である．

継続的な更新が必須　毎日のように情報セキュリティインシデントが報告されているため，コンテンツの継続的なアップデートが必須となっている．このような取り組みを始めることじたい簡単ではないが，継続するのはさらに困難である．したがって，コンテンツの更新に関するワークフローを確立することが課題である．これを敷衍し，コンテンツの開発の前提となる，学習設計を含めた取り組みが必要であると考える．

3. 提案手法

2 節で述べた問題意識を踏まえ，著者らはサイエンティフィック・システム研究会 サイバーセキュリティ・情報倫理 e ラーニング教育の課題解決 WG における活動を通じ，より良いサイバーセキュリティ教育のためのテスト問題を作成するため (1) 「知識」の有無ではなく，判断スキルの習得を前提とする「態度」獲得を目指した，インストラク

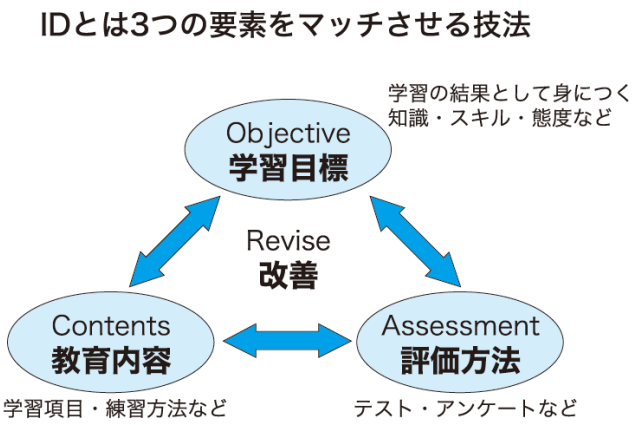

図 1　ID の 3 要素（参考文献 [8] より著者の許諾のもと転載）

ショナル・デザインの考え方を取り入れる (2) 共有リポジトリを構築し，同じ課題を持っている関係者が共同で問題を作成することを提案する．

3.1　インストラクショナル・デザインの採用

著者らは所属機関，企業においてサイバーセキュリティ教育に携わっており，教材の開発と運用を行ってきた．しかしながら，常に教材の開発に全てのリソースを費やすことができるわけではない．セキュリティインシデントが起こる度，または年度末に作問するのが常であり，その “品質” は保証されたものであるとは言えない．また，上述のような事情ゆえ，確立された方針を持って作問しているわけでもない．短期的なプロジェクトであればこれでも良いかもしれないが，セキュリティインシデントは大学の活動に大きな影響を与えるため，その確保のための教育には，一貫した方針を採用することが望ましいと考える．

そこで，e ラーニングによるサイバーセキュリティ教育にインストラクショナル・デザインを導入する．インストラクショナル・デザイン (ID) は，日本語では「教授設計」と言われ，教材設計・開発へのシステム的なアプローチを取るものと定義される．さらに ID による教材設計・開発へのシステム的なアプローチは「Plan-Do-See」の 3 つの段階に分けることができる [7]．これを e ラーニングにおけるテストの作問にあてはめると，「学習目標の明確化 (Plan)」の後に作問 (Do) し，学習目標を達成できたかどうかの評価を行い，改善 (See) することになる．すなわち，我々の行うサイバーセキュリティ教育は単にオンラインコースやテストを受講したという履修主義ではなく「何を学んだか」という習得主義への転換が必要となる．そのためには**図 1** に示す通り，評価方法と学習目標，教育内容を一致させることになる [8]．

我々は本取り組みを通じ，常に学習目標を掲げ，その達成を適切に評価する形で作問を行うこととした．加えて，「知識」の有無ではなく，判断スキルの習得を前提とする「態度」を評価する作問を目指した．すなわち，本取り組み

> 問．ネットサーフィンをしていたら，突然 PC が操作を受け付けなくなり「2 万円を振り込めばアンロックされ，操作ができるようになる」と表示された．この PC は親のものであり，バレたら叱られそうだ．2 万円ならばこっそり払えないことはないが…．次に行うべき行動として適切なものをすべて選べ．
> - 授業料だと思って自分で 2 万円を支払う．
> - スマホを使って，対処方法を検索する．
> - 素直に親に話して 2 万円を払ってもらう．
> - 電源ボタン長押しで PC をシャットダウンする．

図 2　「知識」の有無ではなく，判断スキルの習得を前提とする「態度」獲得を評価する問題の例

全体の学習目標は，(新しいテクノロジや攻撃手法が登場したとしても) サイバーセキュリティ上のインシデントを避ける判断ができる知識 (すべての攻撃と対応パターンを覚える) ではなく，判断しインシデントを最小限に抑える方法を立案，実行できるスキルの習得である．たとえば，**図 2** は「ランサムウェア」を連想させる問題であるが，決して「このようなマルウェアを何と呼ぶか」などの「知識」を問うものではない．インシデントを避けるスキルを持っていれば適切な選択肢を選ぶことができることを意図している．このような，学習目標に一致した作問を行うということである．この作問に加え，問題に対する評価を徹底できれば，2 節で述べた「受講率のみで評価するアリバイ作り的運用」はなくなるであろう．

3.2　共有リポジトリの構築の提案

ここでは，サイバーセキュリティ e ラーニングのための共有リポジトリの構築を提案する．3.1 節で述べた通り，筆者らは所属機関，企業において e ラーニングコンテンツの開発にかかわっており，共通の問題意識を持っている．組織の壁を越え連携することでより良い取り組みが行えるのではないかと考えた．さらに，連携を具現化するプラットフォームとして，次の要件を満たす共有リポジトリの構築を提案する (**図 3**)．

(1)　サイバーセキュリティ教育に関連するテスト問題を公開・共有する

(2)　各組織の事情に合わせテスト問題を選びエクスポートあるいは利用する

(3)　実運用の結果をフィードバックする

これらを満たすことができれば，2 節で述べた「受講者に合わせる」ことは各組織の責任において行うことができる．また，同「継続的な更新」という課題についても，複数の組織の作問を集約することにより，有用なリポジトリとなりうる．

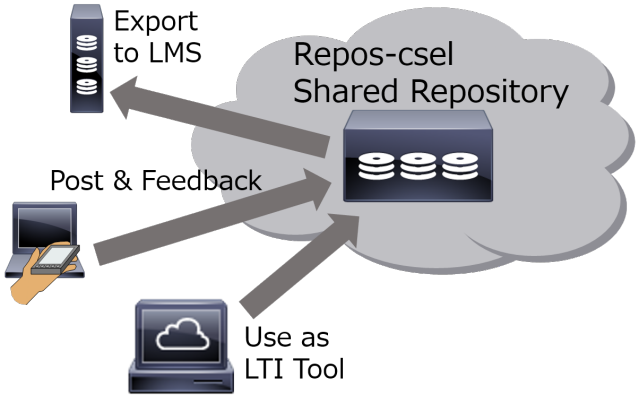

図 3 Repos-csel: Repository for cyber security e-learning 共有リポジトリの概念図

4. 実装と現状

3.2 節で述べた要件について以下の通り検討を行い，Moodle 3.8.1 に StudentQuiz プラグインを導入し共有リポジトリ Repos-csel を構築した．

(1) テスト問題の管理に適しているのは LMS

(2) Moodle は様々な形式で問題をエクスポート可能であり，コース，アクティビティを LTI Tool[9] として利用することも可能

(3) Moodle にはコース管理者でなくてもテスト問題を作成，相互評価できるプラグイン (StudentQuiz)[10] が存在する

4.1 StudentQuiz

StudentQuiz はラッパーズウィル応用科学大学（スイス）の Frank Koch 教授により開発された Moodle プラグインであり，CPLv3 ライセンスで公開されている．同プラグインには以下の機能がある (図 4, 図 5)．

- 学生が自らテスト問題を作成できる
- 問題それぞれに対し評価やコメントを追加することができる
- 作成した問題は問題プールとして共有することができる
- 問題プールの中の問題を取捨選択しテストを受験することができる
- 問題の利用統計を取得することができる
- 問題プールは Moodle の問題バンクの一部であり，StudentQuiz で作成した問題は Moodle 標準の Quiz モジュールで再利用できる

4.2 リポジトリの現状

共有リポジトリ Repos-csel は次のような運用を想定している（Repos-csel には `https://csel.media.hosei.ac.jp/` からアクセスできる．）．

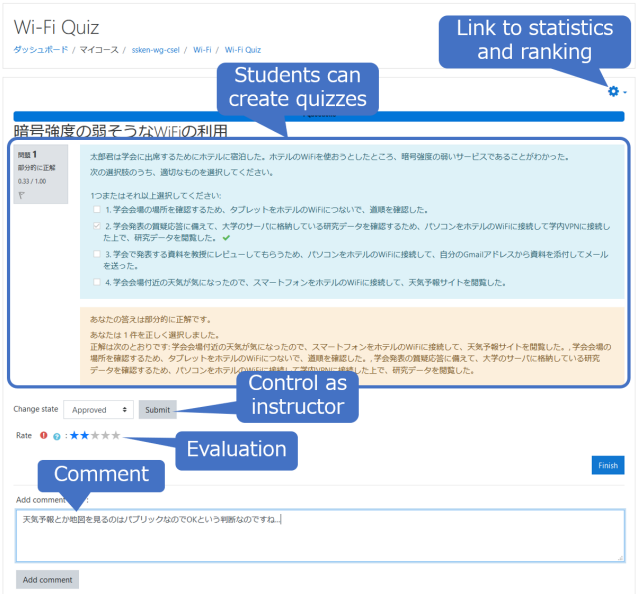

図 4 StudentQuiz のスクリーンショット．学生が問題を作成し相互評価することができるだけでなく，教師ユーザは問題を承認/非承認/編集などの操作が可能になっている．

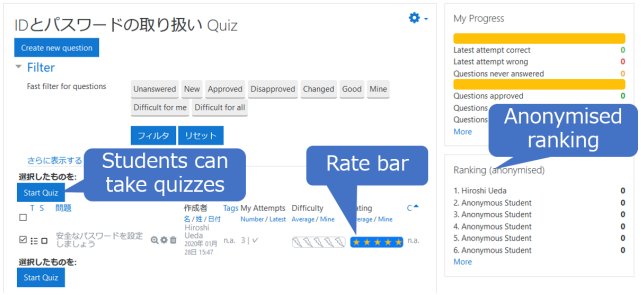

図 5 StudentQuiz のスクリーンショット．学生が問題プールから問題を選択しテストを受験することが可能で，自分に適切な問題を選ぶためのフィルタ，相互評価の統計が表示されている．

- 各機関のサイバーセキュリティ教育実施者が参加し作問する
- 作成した問題は参加者間で共有し，相互に評価する
- 各機関の事情に合わせ問題をエクスポートする，または LTI Tool として使用する

本稿執筆時点ではサイバーセキュリティ・情報倫理 e ラーニング教育の課題解決 WG メンバーが，ID とパスワード，e メール，著作権，Wi-Fi の各トピックに関するテスト問題の作成を次の通り開始している．作問にあたり，各トピックの脅威をリストアップした上で，3.1 で述べた，適切な判断ができるスキルを身につけているかどうかを問う問題となるようにしている．

4.2.1 ID とパスワード

4.2.1.1 脅威：リスト攻撃による不正アクセス

判断スキル パスワードを複数のサービスで使い回した結果事故がおきた．どう対策すべきか？[*2]

作問例 パスワードは忘れないように，どのサービスも同じパスワードを使い回していたが，あるサイトから ID とパスワード漏洩したため，他のサービスで不正ログインの被害にあった．このような事態にあった場合の対策は次のうちどれが適切であるか．

A. ID やパスワードは使い回しせず，Web ブラウザ上でオートコンプリート機能により記憶させておく
B. 家族の名前や生年月日など忘れないようなパスワードにする
C. パスワードは他人から推測されにくい文字列を使用し文字数を多くし，サービスごとに異なる形で用意する

フィードバック オートコンプリート機能自体は，全てのブラウザで安全ではありません（一部を除き，暗号化されずレジストリやブラウザの設定から参照できるものが多数を占めます）．また，家族の名前や生年月日など簡単に推測できるパスワードの場合は，推測され悪用される危険性があります．同様に，同じパスワードを使い回ししていると，万が一知られてしまった場合に危険です．（実際に，パスワード使い回しによる被害が学内でも発生しています．) パスワードは推察されにくい文字列を使用し，文字数を多くするように心がけましょう．

4.2.1.2 脅威：多要素認証に関する理解の不足

判断スキル 多要素認証 (パスワード認証を複数行うことではない)，すなわち別の認証方式の組み合わせで認証することの有用性を認識する．

作問例 A さんは，ある外部の Web システムにおいて，ログイン時に ID とパスワードだけでなく，「父親の名前は？」という質問の答えによる追加認証を用いていた（SMS・e メールへ通知されるワンタイムパスワードは利用していない）．ある時，ID とパスワードが漏洩し，公人である父親の名前を答えにしていた質問による追加認証も突破され，Web システム内の情報を閲覧されてしまった．今後 A さんが認証を強化するための対策を取る場合，より堅固な方法はどれだと考えられますか？強いものから順に並び替えてください．

A. 公人としての父親の名前がバレてしまったので，公人ではない母親の名前をヒントの答えとして設定する．ワンタイムパスワードは使用しない．
B. 家族の名前は容易に推測されてしまうので，秘密の質問を「好きな親友の名前」に変更し，さらに，答えを親友の名前ではなく，好きな車の名前とする．ワンタイムパスワードは利用しない．
C. e メールでワンタイムパスワードが届く認証方式に変更する．通知先のメールアドレスは家族共有のアドレスにする．
D. 指紋認証のある，かつ本人所有の携帯電話へ SMS でワンタイムパスワードが届く認証方式に変更する．

フィードバック 回答後のヒント：複数の要素で組み合わせられる認証を「多要素認証」と呼びます．
各要素には，

- 本人の顔貌，声，指紋など, その人独自の身体的特徴によるアイデンティティ
- 本人のアカウント（メールアドレス）・携帯電話など，その人の所有物によるアイデンティティ（個人の e メールアドレス，SMS で送られるワンタイムパスワードもこれにあたります）．
- あなたが知っている情報（ID とパスワード，家族の名前）によるアイデンティティ

があります．このように，異なる要素で組み合わせた多要素認証は，より強い認証となります．さらに，各要素については，サービス利用者個人だけが所有するほど，漏洩する可能性が少なくなり，より堅固と考えられます．

4.2.2 e メール

4.2.2.1 脅威：添付ファイルによるマルウェア感染

判断スキル 送信元メールアドレス，添付ファイルの拡張子を確認し，開いても良いかどうか判断できるようになる．判断がつかない場合には別の手段で確認することができるようになる．

作問例 1 あなたが受信したメールの送信元メールアドレス，添付ファイルの拡張子が以下の選択肢の通りである場合，開いても良いと思われるものを選択してください（メールアドレスと添付ファイルの拡張子を列挙した選択肢を提示する）．

作問例 2 あなたは「今すぐアカウントを更新」と記載された，添付ファイル付きのメールを受信しました（メール画面のスクリーンショットを提示）．次にどのような行動をすべきでしょうか？最も適切と思われるものを選んでください．

A. メール本文中に記載されている電話番号に確認の連絡をする
B. 同僚や上司に相談する
C. 送信元の公式サイトに同様の情報が掲載されているかどうか確認する
D. 受信したメールに返信して確認する
E. 添付ファイルを開く
F. メールの指示に従い ID とパスワードを入力する

[*2] 「適切なパスワードはどんなものか」から，スキルを問うものに改善した．

4.2.2.2 脅威：情報流出

判断スキル 他人のメールアドレスの流出を防ぎ，機密情報が含まれたファイルを e メールで送信する際に適切な判断ができるようになる．

作問例 1 サークルの全員に e メールで情報を流そうと思います．メールアドレスは次のどこに入れたらいいでしょうか？

A. To:
B. Cc:
C. Bcc:

作問例 2 あなたは機密情報が含まれたファイルを送ろうとしています．安全性が高いと思われる順に並び変えてください．

A. パスワードで保護したファイルを添付して送信し，パスワードは別のメールで送信
B. クラウドストレージなど認証が必要な Web システムにアップロード
C. (パスワードによる保護なしで) ファイルを添付して送信
D. パスワードで保護したファイルを添付して送信し，パスワードは事前に口頭で共有するか，e メールとは別の方法で通知
E. Web サーバにアップロード

4.2.3 著作権

4.2.3.1 情報発信時（レポート，論文執筆，SNS 投稿，ウェブサイト作成）の脅威

判断スキル 情報発信時において（資料を参照しながら）法的根拠に基づいて，その行動が適切である理由を述べられる．不適切な場合はどうすれば適切となるかを提案できる．

作問例 レポート作成をする際に，自分の言いたいことが書いてあるサイトを見つけた

A. サイトの内容をそのままコピペした上で，その下に「この内容は○○というサイトに記載されているものであるが，私はこの内容に激しく同意する」と注意書きを載せた
B. サイトの要約を載せ「この内容は○○というサイトに記載されている」と但し書きをした上で，その後に自分の意見を書いたが，サイトに書かれている内容と概ね同じになった
C. そのサイトを含むいくつかのサイトの意見の要約と URL を載せ，その上で自分がそのサイトの意見に賛成である理由を書いた．
D. そのサイトを読んだ上で自分の言葉で全部書き直し，そのサイトと意見は同じだが，文体は全く違うものとした

4.2.3.2 個人利用時（レンタル DVD，CD のコピー，違法ダウンロード，デジタル万引き）の脅威

判断スキル 個人利用時において（資料を参照しながら）法的根拠に基づいて，その行動が適切である理由を述べられる．不適切な場合はどうすれば適切となるかを提案できる．

作問例 YouTube にある動画を授業で使ったが，その動画がそもそも違法配信だった

A. その動画を使うことをやめて，その動画とよく似た動画を自分で作成して使う．
B. その動画の DVD を購入した上で，引き続き，その動画を使う．
C. YouTube に動画が規約に違反することを報告して削除されたことを見届けたのちに，引き続き，その動画を使う．
D. その動画を使うことをやめ，別の動画を YouTube で探して使う．
E. 動画を使うことをやめて，フリーイラストサイトのイラストを使って説明をすることにする．

4.2.4 Wi-Fi

4.2.4.1 盗聴の脅威

判断スキル 接続している Wi-Fi ネットワークの暗号強度が低い場合にリスクを踏まえた行動ができる．

作問例 太郎君は学会に出席するためにホテルに宿泊した．ホテルの WiFi に接続しようとしたところ，暗号強度の低いサービスであることが分かった．適切な行動を次の選択肢から選択してください．

A. 学会で発表する資料を教授にレビューしてもらうため，パソコンをホテルの WiFi に接続して，自分の Gmail アドレスから資料を添付してメールを送信した．
B. 学会会場付近の天気が気になったので，スマートフォンをホテルの WiFi に接続して，天気予報サイトを閲覧した．
C. 学会発表の質疑応答に備えて，大学のサーバに格納している研究データを確認するため，パソコンをホテルの WiFi に接続して学内 VPN に接続した上で，研究データを閲覧した．
D. 学会会場の場所を確認するため，タブレットをホテルの WiFi に接続し道順を確認した．

5. まとめ

本稿では，大学等におけるサイバーセキュリティ e ラーニングにその有効性，継続性の課題があることを踏まえ，その解決を目指した共有リポジトリの構築を提案した．リポジトリは問題を蓄積するためのものであり，作問にあたり，インストラクショナル・デザインの考え方を取り入れることとした．すなわち，学習目標を掲げ，その達成を適

切に評価するための作問を行うことを目指した．共有リポジトリの実装には，オープンソース LMS である Moodle と StudetQuiz プラグインを採用した．著者らがこれまで取り組んできた，共通 LMS によるサイバーセキュリティ教育と比較した本提案の利点は，各大学等の事情に応じて問題を取捨選択できること，各大学のプラットフォームを活用でき責任分界点が明確であることが挙げられ，より持続的な取り組みを目指すものである．

現在，共有リポジトリ Repos-csel には，ID とパスワード，e メール，著作権，Wi-Fi に関する問題が蓄積されている．どの問題も大学や企業等で実際にサイバーセキュリティ教育に関わっている者がその経験を踏まえ作問したものであり，参考にしていただけるものと確信している．

本取り組みの根底にあるのは，サイバーセキュリティに限らない，「退屈である」「意味がない」といった，e ラーニングに対する悪いイメージを払拭したいという思いである．大学等における e ラーニングは受講が呼びかけられるものの，その明確なインセンティブがない場合が多いことから，e ラーニングコンテンツを改善することが重要と考えた．加えて，同じ問題意識を持つ大学等の関係者が連携するための共有リポジトリを提案した．しかしながら，我々は決して唯一の共有リポジトリを目指しているのではない．人的なものを含め，同様のインスタンスが立ち上がることになれば望外の喜びである．

謝辞　本取り組みに多大なるご尽力を賜わったサイエンティフィック・システム研究会事務局各位に深謝する．

参考文献

[1] 岡村耕二. 九州大学におけるサイバーセキュリティ教育の紹介. 大学 ICT 推進協議会 2016 年度年次大会, p. WD21, Dec 2016.
[2] 中村純, 岡部成玄, 布施泉, 村田育也, 辰己丈夫, 上原哲太郎, 中西通雄, 深田昭三, 多川孝央, 山之上卓. 情報倫理教育. メディア教育研究, Vol. 6, No. 2, pp. S33–S43, 2010.
[3] 岡田仁志. ヒカリ＆つばさの情報セキュリティ 3 択教室. 国立情報学研究所, 2009.
[4] 上田浩, 中村素典, 古村隆明, 神智也. 倫倫姫プロジェクト －学認連携 moodle による多言語情報倫理 e ラーニング－. 情報処理学会論文誌 ディジタルプラクティス, Vol. 6, No. 2, pp. 97–104, Apr 2015. 招待論文.
[5] 岡村耕二. サイバーセキュリティ基礎教育へのシリアスゲームの導入効果に関する研究. 大学 ICT 推進協議会 2017 年度年次大会, pp. WF2–2, Dec 2017.
[6] パナソニックソリューションテクノロジー株式会社. 大学・学校の教職員向けに最適化した「情報セキュリティ教育」, https://www.panasonic.com/jp/business/its/hrd/education/security.html, 2020.
[7] 鈴木克明. 教材設計マニュアル：独学を支援するために. 北大路書房, 2002.
[8] 鈴木克明. インストラクショナルデザインの基礎とは何か：科学的な教え方へのお誘い. 消防研修（特集：教育・研修技法）, Vol. 84, pp. 52–68, 2008.
[9] IMS Global Learning Consortium. Learning tools interoperability, https://www.imsglobal.org/activity/learning-tools-interoperability, 2019.
[10] Frank Koch. StudentQuiz - Empowerig Students, MoodleMoot Global 2019, https://moodle.com/wp-content/events/mootglobal19/StudentQuiz-EmpoweringStudents.pdf, 2019.